UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/086,302	02/28/2002	Alexander Medvinsky	D02643	2065

43471 7590 03/18/2008

Motorola, Inc.
Law Department
1303 East Algonquin Road
3rd Floor
Schaumburg, IL 60196

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	PAPER NUMBER
2137	

NOTIFICATION DATE	DELIVERY MODE
03/18/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing.Schaumburg@motorola.com
APT099@motorola.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/086,302
Filing Date: February 28, 2002
Appellant(s): MEDVINSKY, ALEXANDER

Stewart M. Wiener
Registration No. 46,201
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed January 7, 2008 appealing from the Office action mailed May 7, 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Yang U.S. 6,069,877

Brezak et al. U.S. 2002/0150253

Tung et al. "Public Key Cryptography for Initial Authentication in Kerberos", December 2001, Internet-Draft (updates RFC 1510bis)

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. Claims 1-6, 8, 11-12, 18, 20-22 and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yang United States Letter Patent Number 6,069,877 in view of Brezak et al. (hereinafter Brezak) U.S. Publication Number 2002/0150253.

As per claim 1:

Yang discloses a method for detecting clones (unauthorized duplicate identities) of the client, the method comprising:

forwarding a first signal from a client , the first signal for requesting access to a server; (Col. 2, lines 44-61; Col. 3, lines 39-45 and lines 59-60; Col. 10, lines 43-45)

verifying that the client is authorized to access the server; (Col. 4, lines 4-5)

receiving a second signal from an entity prior to expiration of the time T, the second signal for requesting access to the server, wherein the entity has identifying information identical to the client; (Col. 3, lines 59-67; Col. 4, lines 6-9) and

marking the entity as a possible clone or denying the second request in order to prevent access to the server. (Col. 2, line 45; Col. 4, lines 9-14; Col. 11, lines 21-28)

In addition, Yang discloses if the identification code of the second unit is an apparent duplicate of the first unit and if the first unit has already registered, refusing the registration of the second unit. (Col. 4, lines 9-14) Yang further discloses a base

stations for establishing a session with one or more of the plurality of client units and communicating information between a host computer and one or more mobile communication units. (Col. 2, lines 57-61 and Col. 3, lines 40-45).

Yang does not explicitly disclose a KDC and transmitting an authentication token including an encrypted session key from the KDC to the client, the authentication token for providing access to the server, wherein the authentication token is valid for a time T.

Brezak in analogous art, however, disclose a KDC and transmitting an authentication token including an encrypted session key from the KDC to the client, the authentication token for providing access to the server, wherein the authentication token is valid for a time T. (page 4, paragraph 56, page 5, paragraphs 59-60 and 65) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Yang with Brezak in order to protect the integrity of computer systems and the confidentiality of important data and prevent unauthorized users and malicious attackers from gaining access to computer resource. (page 1, paragraph 2; Brezak)

As per claim 2:

The combination of Yang and Brezak discloses all the subject matter as discussed above. In addition, Brezak further discloses a method wherein the encrypted session key is valid for a designated duration. (Page 4, paragraph 55)

As per claim 3:

The combination of Yang and Brezak discloses all the subject matter as discussed above. In addition, Brezak further discloses a method wherein the designated

duration is for determining the time T for which the authentication token is valid. (Page 4, paragraph 55)

As per claims 4 and 18:

Yang teaches a system for detecting clones of a client within a communication network, the system comprising:

an application server communicably; (Figure 1, Col. 3, line 39)

a client for providing a first request to access the application server; (Figure 1, Col. 3, lines 37-38)

receiving a second request during time T to access the application server, the second request being received from an entity having identifying information identical to the client; (Col. 3, lines 59-67; Col. 4, lines 6-9) and

the KDC denying the second request to prevent the entity from accessing the application server. (Col. 4, lines 9-14; Col. 11, lines 21-28)

In addition, Yang further discloses a base stations for establishing a session with one or more of the plurality of client units and communicating information between a host computer and one or more mobile communication units. (Col. 2, lines 57-61 and Col. 3, lines 40-45).

In addition, Yang discloses if the identification code of the second unit is an apparent duplicate of the first unit and if the first unit has already registered, refusing the registration of the second unit. (Col. 4, lines 9-14) Yang further discloses a base stations for establishing a session with one or more of the plurality of client units and

communicating information between a host computer and one or more mobile communication units. (Col. 2, lines 57-61 and Col. 3, lines 40-45).

Yang does not explicitly disclose a KDC and transmitting an authentication token including an encrypted session key from the KDC to the client, the authentication token for providing access to the server, wherein the authentication token is valid for a time T.

Brezak in analogous art, however, disclose a KDC and transmitting an authentication token including an encrypted session key from the KDC to the client, the authentication token for providing access to the server, wherein the authentication token is valid for a time T. (page 4, paragraph 56, page 5, paragraphs 59-60 and 65) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Yang with Brezak in order to protect the integrity of computer systems and the confidentiality of important data and prevent unauthorized users and malicious attackers from gaining access to computer resource. (page 1, paragraph 2; Brezak)

As per claim 5:

The combination of Yang and Brezak discloses all the subject matter as discussed above. In addition, Yang further discloses a system wherein the entity is a clone. (Col. 2, line 45)

As per claims 6, 24 and 25:

The combination of Yang and Brezak discloses all the subject matter as discussed above. In addition, Yang further discloses a system wherein the identifying

information is a client identifier copied by the clone. (Col. 3, lines 1-4)

As per claim 8:

The combination of Yang and Brezak discloses all the subject matter as discussed above. In addition, Brezak further discloses a system comprising the client deriving a copy of the session key for accessing the application server. (Page 4, paragraphs 56-57)

As per claims 11, 12 and 20:

The combination of Yang and Brezak discloses all the subject matter as discussed above. In addition, Brezak further discloses a system comprising using a key algorithm for authenticating communication between the KDC and the client such that all clients wishing access to the server are required to contact the KDC. (Page 4, paragraphs 56-57)

As per claim 21:

The combination of Yang and Brezak discloses all the subject matter as discussed above. In addition, Brezak further discloses a system wherein a ticket granting server is the server, and the ticket is a ticket granting ticket. (Page 4, paragraphs 56-58)

As per claim 22:

Yang teaches a method for detecting clones in a communication network, the method comprising:

receiving a request during time T to access the KDC, the request being received from an entity with the same identifying information as the authorized client; (Col. 3, lines 59-67; Col. 4, lines 6-9) and

if the request is received during time T, flagging the entity as a possible clone or denying the request to access. (Col. 2, line 45; Col. 4, lines 9-14; Col. 11, lines 21-28)

In addition, Yang further discloses a base stations for establishing a session with one or more of the plurality of client units and communicating information between a host computer and one or more mobile communication units. (Col. 2, lines 57-61 and Col. 3, lines 40-45).

Yang does not explicitly disclose a KDC and providing a an authentication token including an encrypted session key to an authorized client, the authentication token for accessing a KDC, the session key valid for a time duration T.

Brezak in analogous art, however, discloses a KDC and providing a an authentication token including an encrypted session key to an authorized client, the authentication token for accessing a KDC, the session key valid for a time duration T. (page 4, paragraph 56, page 5, paragraphs 59-60 and 65) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Yang with Brezak in order to protect the integrity of computer systems and the confidentiality of important data and prevent unauthorized users and malicious attackers from gaining access to computer resource. (page 1, paragraph 2; Brezak)

As per claim 26:

The combination of Yang and Brezak discloses all the subject matter as discussed above. In addition, Brezak further discloses a system wherein the KDC is the server. (Page 3, paragraph 42)

2. Claims 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yang United States Letter Patent Number 6,069,877 in view of Brezak et al. (hereinafter Brezak) U.S. Publication Number 2002/0150253 further in view of Tung et al. Public Key Cryptography for Initial Authentication in Kerberos, Internet Draft, (hereinafter Tung).

As per claim 9:

The combination of Yang and Brezak discloses all the subject matter as discussed above. Both references do not explicitly disclose a system wherein the encrypted session key is derived using a key agreement algorithm.

Tung in analogous art, however, discloses a system wherein the session key is derived using a key agreement algorithm. (Section 2, paragraph 2)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Yang and Brezak to include a system wherein the session key is derived using a key agreement algorithm. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Tung (Section 2, paragraph 4) in order to enable access to Kerberos-secured services based on initial authentication using public key cryptography.

As per claim 10:

The combination of Yang, Brezak and Tung disclose all the subject matter as discussed above. In addition, Tung further discloses a system wherein the key agreement algorithm is the Diffie-Hellman algorithm. (Section 2, paragraph 3)

(10) Response to Argument

Appellant argued that Yang nowhere discloses **"receiving a second signal from an entity prior to expiration time T"**. The Examiner respectfully disagrees. Yang teaches receiving a session request from the mobile unit; determining the identification code of the mobile unit; determining if there is already a session in progress with any mobile communication unit having the same apparent identification code; and refusing registration to the mobile communication unit **if there already is a session in progress** with any mobile communication unit having the same apparent identification code. (Col. 3, lines 59-67). The examiner interpretes "session" *as "the time during which two computers maintain a connection".* Therefore, Yang discloses receiving a session request and refusing registration to the mobile communication unit if there is already a session in progress with any unit having the same identification code which reads on receiving a request prior to expiration time T which is a particular point in time at which the session ends. Session inherently has beginning and end time, a clone or unauthorized client is detected if a second request with same identification for access is received while the first session is still in progress which is a particular period in time before the end of the session (i.e. prior to expiration time T).

Appellant argued that the determination taught by Yang occurs at any time upon receipt of the second signal, with no reference to any time period associated with the validity or expiration of an authentication token. Yang specifically teaches refusing a second request if the second request is received while there is already a session (i.e. during the time which the first device is connected) with the same identification. Therefore, Yang actually considers a time reference that is while there is already a session with the same identification (i.e. during the session).

Appellant argues that Yang does specifically makes no restriction as to when the attempt to register is received by the network. The Examiner respectfully disagrees. Yang teaches receiving a session request and determining if there is already a session in progress. Therefore, Yang explicitly teaches determining if the session request is received while another session is in progress.

Appellant argues that Brezak also fails to disclose the limitation, of marking the entity as possible clone, or denying the request in order to prevent access to the server when the second request is received prior to the expiration of the time T. Appellant is arguing the references individually, and that one ordinary skill in the art would have been motivated to modify Yang as disclosed above. Brezak discloses a Key Distribution Center (KDC) and transmitting an authentication token including an encrypted session key from the KDC to the client, wherein the authentication token is valid for a time T. Brezak discloses an authentication ticket that contains an encryption key (referred to as a session key), a start and end times of the tickets validity. (page 4, paragraphs 47-48) The KDC sends to client machine a TGT (i.e. authentication token) that contains a

session key (i.e. session key) the valid start and end times for the ticket (i.e. valid for time T). Therefore, Brezak teaches a KDC authenticating a client and sending a ticket with a session key with validity time which meets "*transmitting an authentication token including an encrypted session key from KDC to the client, the authentication for providing access to the server, wherein the authentication token is valid for time T*" as recited in the instant application.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992) In this case, Yang teaches a system wherein a mobile unit being in session with a host computer, base station or other device for exchanging application and/or informational based communication that refuses registration of the mobile unit if there is already a session in progress with same apparent identification code. Brezak teaches an access control to a network using a KDC and generating a ticket that contains encrypted session key, start and end time of the ticket validity. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Yang with Brezak in order to protect the integrity of computer systems and the

confidentiality of important data and prevent unauthorized users and malicious attackers from gaining access to computer resource. (page 1, paragraph 2; Brezak)

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/S. G./
Shewaye Gelagay
Examiner, Art Unit 2137

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132

Conferees:

/G. B./
Supervisory Patent Examiner, Art Unit 2132

Benjamin Lanier
/Benjamin E Lanier/
Primary Examiner, Art Unit 2132